EUCAM Commentary Nº 39, January 2020

COMMENTARY

CESS Centre for European Security Studies
EUCAM
WWW.EUCENTRALASIA.EU

Right to Privacy in Kyrgyzstan

Bermet Zhumakadyr kyzy

Kyrgyz citizens' right to privacy is at risk. In autumn 2019, Kyrgyz news centred mainly on government plans to install in Bishkek Chinese facial recognition cameras that were donated to Kyrgyzstan. These plans were met by strong opposition from civil society. More recently, data from traffic cameras provided by Russia were leaked, leading to controversies about who is actually behind which wheel. It will be important for Kyrgyzstan that its vibrant civil society further shapes the debate, while creating awareness on the importance of privacy rights. What are the challenges in terms of the right to privacy in a low-income country with weak rule of law like Kyrgyzstan?

The issue of privacy rights entered the public discourse in Kyrgyzstan in autumn 2019 with the inauguration of a police command centre in Bishkek. The centre will manage facial recognition cameras installed throughout the city in cooperation with Chinese state-owned enterprise China National Electronic Import and Export Cooperation (CEIEC). The exact number and locations of these cameras are still unknown to the public. Neither is the role of CEIEC beyond providing the hardware, nor whether there will be legal restrictions regarding CEIEC's access to the data collected from the cameras. Should such restrictions exist, it is also unclear how they would be enforced.

Several activists have spoken out against the installation of cameras with facial recognition capacities. The Civic Control Committee, comprised of over 70 NGOs that monitor various government projects, has called for a moratorium on the use of facial recognition technology. In an interview with *Azattyk*, Committee member Dinara Oshurakhunova expressed her concerns about the use of such cameras without properly ensuring people's safety first: 'It is well known that corruption is blossoming in our legal system. There are well known cases where law enforcement representatives committed crimes in cooperation with criminals. Who knows how the data of six million Kyrgyz people could be used in this case?'

According to the Kyrgyz government, facial recognition cameras are in line with the government's strategy to enhance road safety, reducing traffic violations and car accidents. For the so-called 'Safe City' project, the Kyrgyz government turned down an offer from Chinese company Huawei, signing instead a deal with Russian company Vega to install traffic cameras in September 2018. Vega's cameras laid the infrastructural foundations for CEIEC's surveillance system. Facial recognition technology in public spaces opens the door to indiscriminate surveillance and blanket collection of data on everyone who walks past these cameras. If this data is not erased, it becomes a permanent record of people's habits and movements, which could be accessed and misused by the owner of the technology if not properly regulated. The issue of privacy rights is larger than the surveillance potential offered by facial recognition cameras.

Corporations and governments around the world collect data, which can be retained permanently, on Internet users through facial recognition cameras, social networks, systems, devices, etc. While this might seem similar to what is happening in Kyrgyzstan, in Western democracies the issue of privacy rights has been on the agenda for quite some time, and citizens' rights are better protected through rule of law and democracy. In Kyrgyzstan, where corruption and clientelism are common practice, people's right to privacy is at a much greater risk as Kyrgyz authorities are much more easily influenced by local power brokers, companies, foreign governments, and global corporations. Whereas the debate of 'security versus privacy' is similar in Western democracies and Kyrgyzstan, with governments arguing that cameras and other surveillance technology serve solely to enhance public safety, Kyrgyz citizens have fewer legal safeguards and instruments to protect their privacy.

There have already been several cases of mishandling of private data by the Kyrgyz authorities. In November 2019, it was revealed that the State Registration Services Agency has been selling citizens' data to financial organisations, telecommunication companies, and banks since December 2017. According to the Agency, the selling of passport data is considered to be a state service which is provided upon payment. Another prominent case of misuse of private data is Samara-gate – citizens' personal data were used by current President Sooronbai Jeenbekov to win the 2017 presidential elections.

In addition to the threat of misuse of private data by the Kyrgyz government and businesses, there is a danger of misuse of data by foreign governments. Well-resourced intelligence agencies in *Western democracies* collect data on foreign nationals, including Kyrgyz citizens. The collection of data at a mass scale by the NSA unveiled by Snowden in 2011 led to massive public outrage in Western democracies. But in the United States (US), for example, the public was outraged that the government was spying on 'its own citizens', not necessarily that it was spying on other countries.

Another foreign government that has been violating Kyrgyz people's right to privacy is *China*. China has started to expand its influence in the region, especially with its Belt and Road Initiative. CEIEC, the Kyrgyz government's partner in the installation of face recognition cameras, also installed cameras for a massive surveillance project in Xingjian province in China.

Russia also has a role, since it was Russian company Vega that installed the first cameras setting up the infrastructure for CEIEC. Kyrgyzstan has a tendency of closely following Russia in terms of laws and regulations. Although China's digital penetration in the region is increasing, Russia still has a very strong influence due to a shared history and mentality when it comes to human rights and democracy. Privacy is a low priority among the general public in Russia, and this is mirrored in current public attitudes toward the issue in Kyrgyzstan.

The primary financial beneficiaries are *corporate giants* such as Google, Facebook and Microsoft that have been drivers of mass data collection. These companies make huge profits thorough the collection of private data that users provide knowingly or otherwise. These companies do not discriminate whether a country is low-income or not, or whether it has a weak rule of law system or not. The difference in countries like Kyrgyzstan is that people have fewer means to safeguard their privacy. Unlike the European Union (EU), Kyrgyzstan does not have General Data Protection Rules.

Kyrgyzstan has a comparatively vibrant civil society consisting of NGO representatives, social justice activists, academics, artists, and so on. It was Kyrgyz civil society that vehemently stood up against and stopped the Russian copy-paste 'foreign agent bill' of 2014 from being approved. Among others, the tech-focused public fund Civil Initiative on Internet Policy, an NGO focusing on information technologies-related law and policy, could be a platform to begin discussions on privacy rights. The fund and the Civic Control Committee were among the first and few to comment on and react to the news of the installation of facial recognition cameras in Bishkek. Unfortunately, there are not many people with a tech background involved in civic issues, while human rights defenders and most NGOs lack the technical expertise. Other powerful allies could be investigative journalists who have uncovered instances of misuse of private data by the authorities. Ideally, new initiatives would bring activists, journalists and NGOs with the technical capacity together to work around an agenda of awareness-raising and safeguarding privacy.

Furthermore, civil society from Western democracies could help civil society in Kyrgyzstan (and in other young democracies with weak rule of law) by spurring debate given their experience in addressing these issues. The recently released Human Centric Digital Manifesto for Europe by the Open Society European Policy Institute and the European Consumer Organisation says that the European Union 'has a unique opportunity to shape the digital transformation and position itself as a global leader and ambitious norm-setter that puts people and the public interest back at the centre of the 21st century revolution'. Even though European countries have their own challenges regarding data privacy regulations, their experience could be invaluable to countries such as Kyrgyzstan.

The installation of facial recognition cameras in Bishkek has led to a first short-lived spark of discourse on citizens' privacy rights. But facial recognition cameras are only the tip of the iceberg. Privacy rights are under threat given the use of other technologies by Kyrgyz authorities, often in cooperation with local businesses, foreign governments, and big tech corporations. As a shared sense of understanding of the implications of technological advancements on privacy rights is yet to be formed, it is crucial that civil society take the lead and shape public discourse.

Author:

Bermet Zhumakadyr kyzy was a 2019 autumn fellow at the EUCAM fellowship programme of the Centre for European Security Studies (CESS), Groningen, The Netherlands.

OPEN SOCIETY FOUNDATIONS

Supported by a grant from the Open Society Foundations.